UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/726,180	11/29/2000	Masao Kasahara	83308.0001	5969

26021	7590	04/23/2004

HOGAN & HARTSON L.L.P.
500 S. GRAND AVENUE
SUITE 1900
LOS ANGELES, CA 90071-2611

EXAMINER
AKPATI, ODAICHE T

ART UNIT	PAPER NUMBER
2135	5

DATE MAILED: 04/23/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

	Application No.	**Applicant(s)**	
Office Action Summary	09/726,180	KASAHARA, MASAO	
	Examiner	**Art Unit**	
	Tracey Akpati	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-12* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-12* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on <u>29 November 2000</u> is/are: a)☒ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☒ All   b)☐ Some * c)☐ None of:

      1.☒ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage
application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date <u>2</u>.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

DETAILED ACTION

Claim Objections

Claims 4 and 9 are objected to because of the following informalities:

With respect to Claim 4, the phrase "comprising a second polynomial to a product" is unclear to the examiner at to what the applicant is trying to claim. The examiner urges the attorney to use clear language so as to illuminate the claimed invention. Furthermore, the word "polynomial" is misspelled. All further occurrences of this word should be corrected appropriately. Also, the applicant talks about a third secret key but does not previously in the claims talk about a second secret key. Appropriate corrections regarding this issue would be greatly appreciated.

With respect to Claim 9, the phrase "wherein said cyphertext is an evaluation of a first polynomial at the plaintext" is unclear to the examiner. The word "ciphertext" is also misspelled. All other occurrences of this word should be corrected appropriately.

Because the examiner cannot decipher the phrases of Claim 4, "comprising a second polinomial to a product", for the purpose of applying prior this phrase is ignored. With respect to Clam 9 "evaluation of a first polynomial at the plaintext", for the purpose of applying prior art, the word "evaluation" is taken to mean "function" and the phrase "at the plaintext" is ignored.

Appropriate correction of the above objections would be greatly appreciated.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1, 5, 6, 8, 11, 12 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Uchiyama et al (6480605 B1).

With respect to Claim 1, the limitation of "a step for multiplying the cyphertext by a first

secret key" is met on column 10, lines 52-67; and "a step for permuting the sequence of the sub-

elements in the cyphertext in such a way that said sub-elements are separated into a part

corresponding to the plaintext and noise" is met on column 10, lines 36-45. The random number

in the reference represents the noise. The random number is combined with the message during

encryption. After decryption, the random number is not longer present (column 10, lines 63-67

and Fig. 1). Hence, this suggests that the random number must have been extracted from the

ciphertext during the decryption process. Therefore, it would have been obvious to one of

ordinary skill in the art at the time the invention was made to have the noise separated from the

plaintext message as part of the decryption process because this separation step of plaintext from

noise allows the original message to be retrieved.

With respect to Claim 5, the limitation of "obtaining a power root of said product" is met

by Fig. 1.

With respect to Claim 6, the limitation of "sending to said digital information processing device a computer program including a sub-program for multiplying the cyphertext by a first secret key, and a sub-program for permuting the sequence of the sub-elements in the cyphertext in such a way that said sub-elements are separated into a part corresponding to the plaintext and noise and making said digital information processing device decrypt the cyphertext according to said computer program" is met on column 10, lines 48-67. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have the noise separated from the plaintext message as part of the decryption process because this separation step of plaintext from noise allows the original message to be retrieved.

With respect to Claim 8, its limitation is similar to Claim 1, except for the fact that it is claiming a decryptor that performs the functions described in Claim 1. Because of the existence of the steps described in Claim 1 in the reference, the existence of a decryptor, a device that performs these steps is obvious.

With respect to Claim 11, its limitation is similar to Claim 1, except for the fact that a recording medium that performs the decrypting functions is claimed. Because of the existence of the steps described in Claim 1 in the reference, the existence of any device e.g. a recording medium that incorporates this invention is obvious.

With respect to Claim 12, its limitation is similar to Claim 1, except for the fact that a propagating signal that performs the decrypting functions is claimed. Because of the existence of the steps described in Claim 1 in the reference, the existence of any signal that incorporates the decryption steps of the invention is obvious.

Claims 2, 3, 7, 9 and 10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Uchiyama et al (6480605 B1) in view of Raike (5799088).

With respect to Claim 2 and 7, all the limitation is met by Uchiyama et al except for the limitation disclosed below.

The limitation of "wherein said cyphertext is obtained by substituting the plaintext for an indeterminate of a first polynomial" is met by Raike on column 13, lines 9-29. The mixture generator disclosed in the reference is used in the encryption process (column 11, 29-31 and Fig. 2) to get the ciphertext.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Raike within the system of Uchiyama et al because polynomials are well known means used in encryption schemes.

With respect to Claim 3, all the limitation is met by Uchiyama et al except the limitation disclosed below.

The limitation of "wherein said first secret key is one of powers of a primitive root of a primitive polynomial in the finite extension field" is met by Raike on column 10, lines 51-54 and on column 22, lines 52-58.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Raike within the system of Uchiyama et al because polynomials are well known means used in encryption schemes.

With respect to Claim 9, all the limitation is met by Uchiyama et al except for the limitation disclosed below.

The limitation "wherein said ciphertext is an evaluation of a first polynomial at the plaintext" is met by Raike on column 14, lines 45-52 and on column 15, lines 3-7.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Raike within the system of Uchiyama et al because polynomials are well known means used in encryption schemes.

With respect to Claim 10, the limitation of "a means for multiplying said part corresponding to the plaintext by a third secret key comprising a second polynomial into a product and for obtaining a power root of said product" is met by Uchiyama et al on column 8, lines 36-40 and on Fig. 1. Uchiyama et al however does not disclose the below limitation.

The limitation of "wherein said multiplication means multiplies the cyphertext by one of powers of a primitive root of a primitive polynomial in the finite extension field as the first secret key" is met by Raike on column 10, lines 51-54 and on column 22, lines 52-58.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Raike within the system of Uchiyama et al because

multiplying the ciphertext with the primitive root of a primitive polynomial allows for the

plaintext to be retrieved.

Claim 4 is rejected under 35 U.S.C. 103(a) as being unpatentable over Uchiyama et al

(6480605 B1) in view of Gutowitz (5365589).

With respect to Claim 4, all the limitation is met by Uchiyama et al except for the

limitation disclosed below.

The limitation of "multiplying said part corresponding to the plaintext by a third secret

key..." is met by Gutowitz in the abstract. The secret keys disclosed are used to encrypt the

message. It further states that decryption merely uses the methods similar to the encryption

steps. This means that the keys used to encrypt are also used to decrypt. Also, we can gather

that more than one key is used to encrypt, hence more than one key would be used to decrypt.
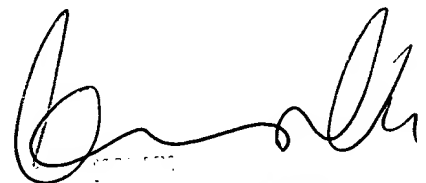
It would have been obvious to one of ordinary skill in the art at the time the invention

was made to combine the teachings of Gutowitz within the system of Uchiyama et al because

multiplying the part corresponding to the plaintext with a secret key allows for the plaintext to be

retrieved.

Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Tracey Akpati whose telephone number is 703-305-7820. The

examiner can normally be reached on 8.30am-6.00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Kim Vu can be reached on 703-305-4393. The fax phone number for the

organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent

Application Information Retrieval (PAIR) system. Status information for published applications

may be obtained from either Private PAIR or Public PAIR. Status information for unpublished

applications is available through Private PAIR only. For more information about the PAIR

system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR

system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

OTA